Squeezing the cloud

Military, intell organizations look at enhanced data storage and distribution capabilities

BY JOHN EDWARDS

Virtually all defense organizations and intelligence agencies are turning toward cloud computing for everything from satellite imagery to telecom traffic to Web content. For these applications and many others, the focus is on building private cloud systems that can cost effectively store and efficiently distribute multiple petabytes of data to endpoints worldwide.

John Thielens, chief architect of cloud services at Axway, a provider of data security services to the Defense Department, said it's hard to build a financially wasteful cloud environment. "It's the main benefit of adopting cloud [technology]," he said, "[Adopters are] saving money through massive economies of scale and increasing the use of commercial, off-the-shelf products, as opposed to undertaking expensive, specialty, old-fashioned, government-style development."

Dan DelGrosso, director of Naval Networks and Enterprise Services, said no matter how cloud computing is approached, it promises to save money. "For the Navy, there would be at least two general cost models: utility and fixed price," DelGrosso said. Utility cloud computing is billed by the contractor on a usage basis while a fixed-price agreement supplies a packaged set of cloud services for a specific period. "If both cost models support so-called 'cloud elasticity,' then either cost model will save the Navy money," he said. "This is true, since the cost of expanding capacity, upgrading and patching applications, and continually updating security, will be absorbed by the cloud provider."

Beyond generating cost savings, a cloud environment typically operates more responsively than the technologies it replaces. "The main differentiator between legacy and cloud-based storage deployments resides in the speed and flexibility that storage requests can be met," said Tom Houston, chief technologist at Hewlett-Packard Enterprise Services. "The near real-time flexibility and speed [with which] cloud-based storage can be provisioned and made available to end-users is a major differentiator when comparing cloud computing to legacy infrastructure deployments and procurement processes," he added.

An Air Force technician maintains computer networks at the Joint Network Operations Control Center at Camp Victory, Iraq. Nearly all defense organizations and intelligence agencies are turning toward cloud computing to handle the large volumes of data they store and share.

EFFICIENT AND SECURE DISTRIBUTION

DOD and intelligence agency adopters are looking for cloud computing technologies and approaches that can efficiently deliver data to users located almost anywhere. However, network service must be configured and scaled to each user's needs and limitations. "The network has to be smart enough to recognize whether the user has a bandwidth-limited device and then adjust what it sends through accordingly," said John Garing, former Defense Information Systems Agent CIO officer and currently vice president of ViON, a systems integrator. "It depends on what device is being used, who is using it and whether the user is in Crystal City [Virginia] or Kandahar."

Security, meanwhile, must be maintained throughout the cloud environment. Garing said cloud access can be both protected and optimized by creating "community clouds" for specific groups of end users based on individuals' needs and security clearances. Cloud access can also be filtered trough a variety of security oriented processes, such as "layered defenses, layered demilitarized zones and strong and robust cross-domain information sharing," Garing said.

Defense and intelligence cloud computing can take advantage of a strong existing network security foundation, Thielens said. "One of the nice things about the government in general is that there's a very mature ecosystem for dealing with credentialing, authentication and authorization problems at the HSPD-12 level, but especially for defense and intelligence agencies, which have more stringent identity management infrastructures," he said. "I think that's the backbone of how you deal with security, access rights and security tracking — at least at the user level." ■